	CHAPTER: Fiscal Management	**POLICY**: *PCI DSS* **PAGES**: 3
	SUBJECT: *PCI DSS Policy*	
RELATED POLICIES: Information Services Policy Resolution 257-1997	**ENABLING RESOLUTION**: **RESOLUTION DATE**: **REVISED RESOLUTION & DATE**:	
OFFICE WITH PRIMARY RESPONSIBILITY: Finance/ITS		

I. Statement of Purpose

The purpose of this policy is to define the guidelines for accepting and processing payment cards and storing personal cardholder information. The policy will help to ensure that cardholder data supplied to Sedgwick County is secure and protected. Sedgwick County Departments will comply with data security standards set out by Sedgwick County and in accordance with the Payment Card Industry Data Security Standards (PCI DSS).

II. Policy

A. The principle of 'least privilege' will be utilized to restrict access to cardholder account information. Positions requiring specific levels of data access will be provided in written form by the Department Head or designee, to the Director of Accounting. For employees without a "need to know", payment card account numbers will be masked to protect account information. The last four digits are the maximum number of digits to be retained and displayed.

B. Each authorized staff member will maintain password(s) for all systems associated with payment card equipment and data. **Passwords are individual specific and are not to be disseminated or shared**.

C. The following payment card information will be stored and locked in the absence of authorized staff and during non-business hours as follows:
   a. Business;
   b. Name.

   Full account number and expiration date will not be retained past the period of the transaction. This information will immediately be destroyed.

D. **The three (3) or four (4) digit card verification value (i.e., CVV2) is never stored in any format past the period of the transaction. This information will be destroyed immediately.**

E. Payment card equipment and card holder data will be secured at all times with access permitted for authorized staff members only. Authorized staff leaving the work area will, secure and lock all payment card information. Unauthorized personnel are not permitted in the secured work area

unless accompanied by an authorized staff member. Visitors from other agencies, departments and the general public are not permitted in this secured area. If a breach of security is encountered, the authorized staff member will immediately notify the Department Head and the PCI-DSS Team Member.

F. Under no circumstances will it be permissible to obtain payment card information or transmit payment card information by email or telephone without written permission from the Director of Accounting.
G. Cardholder data is never released in any form unless there is a legitimate business purpose approved and authorized by Director of Accounting.
H. Cardholder data will be destroyed immediately following the transaction.
I. Payment card policies and/or procedures are subject to audit and/or modification at any time.
J. Payment card transactions are subject to audit at any time by the Department Head, PCI-DSS Team Member, Sedgwick County and Payment Card Industry Compliance personnel.
K. Participation in Sedgwick County's Security Awareness training is mandatory.
L. Violations of Sedgwick County's Payment Card Policies and/or Sedgwick County's Payment Card Procedures will result in immediate disciplinary action up to and including termination of employment.

Data Storage and Destruction

The following processes must be followed for all data storage and destruction:

A. Hardcopy containing cardholder data will be destroyed immediately after processing by placing hardcopy materials in secured shredding bins.
B. All electronic media containing cardholder information will be contained in confidential formats accessible to authorized staff only.

Process for Responding to a Security Breach

In the event of a breach or suspected break of security, authorized staff must immediately perform the following steps:

1. Contact the Department Head and Director of Accounting. These individuals will provide further instructions which will include measures that will preserve electronic evidence.
2. The Director of Accounting will coordinate the investigation, document and remediate the situation in partnership with the Department Head.
3. All investigation and collection of evidence will be coordinated by the Director of Accounting. To prevent alteration of the compromised system or systems, authorized staff is instructed to act as follows:
    a. Do not switch off the compromised machine.
    b. Do not attempt to isolate the compromised system(s) from the network by unplugging the network connection cable.
    c. Do not log on to the machine and/or change passwords.
    d. Report suspicious activity to the Department Head and Director of Accounting.

Stolen Payment Cards

If the payment card system identifies a card as stolen authorized staff is to notify the Sedgwick County Sheriff's Office and the Director of Accounting.

IV. DEFINITIONS

A. *Cardholder Data*: Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, Card Validation Code CVC 2 (MasterCard), Card Verification Value CVV2 (VISA), or Card member ID (Discover).
B. *PCI DSS*: The *Payment Card Industry Data Security Standard* – A set of comprehensive requirements for enhancing payment account data security, developed by the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.
C. *Principle of Least Privilege*: The principle of 'least privilege' involves assigning individuals access on a 'need to know' basis.
D. *PCI-DSS Team*: A cross-functional team with the following members – Director of Accounting (Finance), Principal Accountant – Cash Management (Finance), Contracts & Compliance Officer (ITS), IT Security Manager (ITS), and PCI Officer (ITS).
E. *Unauthorized Person*: An individual who during the normal course of business/assigned duties does not have a need to access the payment card data.